



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/451,160	11/30/1999	STEVEN R. BOAL	80.142-002	8692

7590 02/14/2005

RONALD P. KANANEN, ESQ.  
RADER, FISHMAN & GRAUER P.L.L.C.  
1233 20TH STREET N.W.  
SUITE 501  
WASHINGTON, DC 20036

EXAMINER

MYHRE, JAMES W

ART UNIT	PAPER NUMBER
----------	--------------

3622

DATE MAILED: 02/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/451,160

Applicant(s)

BOAL, STEVEN R.

Examiner

James W Myhre

Art Unit

3622

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 23 December 2004.
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-18 and 22-46 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-18 and 22-46 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Response to Amendment***

1. The amendment filed on December 23, 2004 is sufficient to overcome the 35 U.S.C. 102/103 rejections in view of the Stewart (5,835,601) and Payne et al (5,715,314) references. The amendment provided amended drawings, an amended abstract, an amended specification, and amended Claim 1-7, 9, 11, 13-17, 24, 26-32, 34, 36, 38-42, and 44-46. The currently pending claims considered below are Claims 1-18 and 22-46.

### ***Drawings***

2. The drawings were received on December 23, 2004. These drawings are acceptable except as indicated below.

The drawings are objected to because in Figure 5, Item 132, the "No" arrow should be pointing out from the box, not into the box. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief

Art Unit: 3622

description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### ***Specification***

3. The new abstract of the disclosure and amended specification are acceptable and have been entered in the application.

### ***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 24 and 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Barnett et al (6,321,208).

Claim 24: Barnett discloses a method for secure coupon distribution, comprising:

- a. associating a URL (Internet website address) with a coupon with an appended promotional code (bar code)(col 6, lines 29-51 and col 7, lines 21-35);
- b. invoking use of the URL with a browser to enable the user to redeem the coupon (col 6, lines 29-51 and col 11, lines 33-43); and
- c. disabling future use of the invoked URL (by deleting the coupon)(col 11, lines 44-51).

Claim 25: Barnett discloses a method for secure coupon distribution as in Claim 24 above, and further discloses the user selecting the coupon by clicking (mouse input) on the displayed coupon or an object difference than the displayed coupon (col 8, lines 52-67).

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-18, 22, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barnett et al (6,321,208) in view of Stewart (5,835,061).

Claim 1: Barnett discloses a method for secure coupon distribution as in Claim 24 above, but does not explicitly disclose collecting a device ID from the client system and transmitting a selected coupon to the client device based upon the device ID

Art Unit: 3622

without being able to identify the user. However, Stewart discloses a similar method for distributing promotional messages (e.g. coupons) to a client device by collecting device information (mobile unit ID) about a client device (col 3, lines 56-60); associating the device ID with device information at a main server (col 4, lines 1-3); selecting a coupon (promotional message) according to the device ID based on the device information; and transmitting the selected coupon to the client device (col 8, lines 12-19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the device ID to identify the user's device in Barnett. One would have been motivated to use the device ID instead of a user ID in order to prevent the user in Barnett from receiving multiple copies of the coupon by registering multiple user IDs. Since Barnett only allows one copy of the coupon to be delivered and printed at a device (identified by its web address), if the system only checked user IDs, a user could register multiple user IDs with the system and receive multiple coupons - - defeating the security measures outlined by Barnett.

Claim 2: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 1 above, and Barnett further discloses the device information including at least one of a postal zip code and a state in which the user resides (col 4, lines 8-16 and 34-37).

Claim 3: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 1 above, and Stewart further discloses associating the device ID with a remote client system by the main server system (col 4, lines 1-3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for the main server in Barnett to identify the user device by associating the device ID with the user device. One would have been motivated to do such association at the main server in Barnett in order to allow the “efficient, low cost, zip-code/lifestyle/lifestage or household targeted coupon distribution system to tailor the incentives to each user” as discussed in Barnett. The Examiner notes that a system which tailors the incentives to a user based on zip code or household does not inherently identify the specific user.

Claim 4: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 3 above, and Barnett further discloses the client system being able to print the transmitted coupon (col 7, lines 6-11).

Claims 5 and 6: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 3 above, and Stewart further discloses the client system submitting a request including the device ID to the main server (col 4, line 65 – col 5, line 6) without intervention by the remote user (col 5, lines 34-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include the device ID with the user request in Barnett (col 9, lines 34-41). One would have been motivated to include the device ID with the request in order to identify

the correct device to which to send the response across the network. The Examiner notes that this (using automatically transmitted device IDs) is the common method of identifying initiators of requests across computer networks.

Claim 7: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 5 above, and Barnett further discloses transmitting the request without any intervention by the user (automatic updating)(col 5, lines 35-39 and col 9, lines 29-33).

Claim 8: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 7 above, and Stewart further discloses the transmitting step occurs at predetermined intervals (beacon signals)(col 4, lines 10-19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to perform the automatic updating (transmitting step) in Barnett at predetermined intervals. One would have been motivated to perform this step periodically in order to ensure the user had the most up-to-date coupon information.

Claims 9 and 10: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 3 above, but neither of the references explicitly disclose that the graphical user interface on the client device uses icons which may also flash to indicate the availability of new coupons. However, Official Notice is again taken that the use of icons, graphics, colors, animation, etc. to attract the viewer's attention on graphical user interfaces is well known in the computer arts, and their use would have been obvious to



Art Unit: 3622

one having ordinary skill in the art at the time the invention was made. In support of this Official Notice, the Examiner previously provided excerpts from two HTML textbooks from 1996 to show that, not only was it well known to “flash” parts of a web page to attract the user’s attention, but that the “Blink” command was also one of the standard commands in the programming language (Graham, “The HTML Sourcebook, Second Edition, A Complete Guide of HTML 3.0”, 1996, pp 233-234)(Lemay, “Teach Yourself Web Publishing with HTML 3.0 in a Week”, 1996, pp 183). Therefore, one would have been motivated to use icons, flashing or otherwise, to notify the user of the Barnett system in order to attract their attention more easily.

Claims 11 and 12: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 3 above, but neither reference explicitly discloses that the coupon data is encrypted before it is sent to the client system nor that the client system will also encrypt the coupon data upon receiving the data from the remote server. Official Notice is taken that it is old and well known within the computer and data encryption arts to encrypt data being sent over unsecured networks using a plurality of encryption methods in order to provide a higher level of security to the data. In support of this Official Notice the Examiner previously provided Chapter 15 from a cryptography textbook from 1996 to show that not only was double encryption a well known method to further protect data, but triple encryption and other multiple encryption schemes were also well known and used in the art (Schneier, “Applied Cryptography, Second Edition”, 1996, pp 357-368). Therefore it would have been obvious to one having ordinary skill in

Art Unit: 3622

the art at the time the invention was made to encrypt the coupon data in Barnett prior to transmitting the data over an unsecured network, such as the Internet as disclosed by Barnett, in order to prevent unauthorized interception of the data. It also would have been obvious to one having ordinary skill in the art at the time the invention was made to use a local encryption method to further encrypt and protect the encrypted data received from the remote server. One would have been motivated to further encrypt the coupon data in Barnett locally in this manner in order to prevent unauthorized disclosure of the selected coupons to other persons who may use the client device (e.g. other family members, co-workers, etc.).

Claim 13: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 12 above, and Barnett further discloses generating a printed version of the selected coupon (col 7, lines 6-11). It is inherent that the client device must decrypt the encrypted coupon data before printing the coupon.

Claim 14: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 3 above, both Barnett and Stewart further disclose displaying at least a portion of the advertisement (coupon) to the user of the client device (Barnett, col 9, lines 54-58)(Stewart, col 4, lines 5-7 and col 7, lines 12-20).

Claim 15: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 14 above, and Barnett further discloses selecting one of the plurality of coupons as a function of a selected subcategory of coupons available on the client system (col 10, lines 1-16).

Claim 16: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 2 above, and Barnett further discloses tracking the user's actions on the client device and maintaining a database at the main server of coupons selected and redeemed by the user (col 10, lines 51-57).

Claim 17: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 16 above, and Barnett further discloses determining a sponsor identification of a displayed coupon (col 11, lines 25-29).

Claim 18: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 16 above. While it is not explicitly disclosed that the data being sent to the main server about the tracked user's actions is encrypted, it would have been obvious to do so for the same reasons discussed in reference to Claims 11 and 12 above.

Claim 22: Barnett discloses a method for secure coupon distribution as in Claim 24 above, but does not explicitly disclose collecting a device ID from the client system and transmitting a selected coupon to the client device based upon the device ID

Art Unit: 3622

without being able to identify the user. However, Stewart discloses a similar method for distributing promotional messages (e.g. coupons) to a client device by collecting device information (mobile unit ID) about a client device (col 3, lines 56-60); associating the device ID with device information at a main server (col 4, lines 1-3); selecting a coupon (promotional message) according to the device ID based on the device information; and transmitting the selected coupon to the client device (col 8, lines 12-19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the device ID to identify the user's device in Barnett. One would have been motivated to use the device ID instead of a user ID in order to prevent the user in Barnett from receiving multiple copies of the coupon by registering multiple user IDs. Since Barnett only allows one copy of the coupon to be delivered and printed at a device (identified by its web address), if the system only checked user IDs, a user could register multiple user IDs with the system and receive multiple coupons - - defeating the security measures outlined by Barnett. However, neither reference explicitly discloses that the coupon data is encrypted before it is sent to the client system nor that the client system will also encrypt the coupon data upon receiving the data from the remote server. Official Notice is taken that it is old and well known within the computer and data encryption arts to encrypt data being sent over unsecured networks using a plurality of encryption methods in order to provide a higher level of security to the data. In support of this Official Notice the Examiner previously provided Chapter 15 from a cryptography textbook from 1996 to show that not only was double encryption a well known method to further protect data, but triple encryption and other multiple encryption

Art Unit: 3622

schemes were also well known and used in the art (Schneier, "Applied Cryptography, Second Edition", 1996, pp 357-368). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the coupon data in Barnett prior to transmitting the data over an unsecured network, such as the Internet as disclosed by Barnett, in order to prevent unauthorized interception of the data. It also would have been obvious to one having ordinary skill in the art at the time the invention was made to use a local encryption method to further encrypt and protect the encrypted data received from the remote server. One would have been motivated to further encrypt the coupon data in Barnett locally in this manner in order to prevent unauthorized disclosure of the selected coupons to other persons who may use the client device (e.g. other family members, co-workers, etc).

Claim 23: Barnett and Stewart disclose a method for secure coupon distribution as in Claim 22 above. While neither reference explicitly discloses that the encrypted coupon data would be decrypted to recover the selected coupon, it is inherent that the client device must decrypt the encrypted coupon data before displaying or printing the coupon.

8. Claims 26, 36-38, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart (5,834,061) in view of Ogasawara (6,123,259).

Claims 26 and 44: Stewart discloses a system and method for secure coupon distribution, comprising:

- a. collecting device information (device ID) about a client device which is insufficient to identify the specific user (col 3, lines 56-60);
- b. associating the device ID with device information at a main server (col 4, lines 1-3);
- c. selecting a coupon (promotional message) according to the device ID based on the device information; and
- d. transmitting the selected coupon to the client device (col 8, lines 12-19).

While Stewart discloses that the remote device only transmits its device ID, it is also disclosed in most embodiments that the system “knows” the identity of the user to which the remote device has been assigned (through prior registration, etc.). Therefore, when associating the device ID with the device information (step b above), the main server may be able to ascertain the identity of the specific user (or at least the assigned user) of the remote device. However, it is also disclosed that the system has “the ability to provide customized messages based on the location of the active access point” (i.e. the location of the remote device) such as “a user accessing a network through an access point in a hotel may be provided information about promotions offered by that hotel or other affiliated hotels, airlines, car rental agencies or other providers of goods or services” (col 8, lines 12-18) There are other similar systems using remote shopping devices, such as Ogasawara who discloses that “each terminal is assigned a unique terminal ID and all communications between that terminal and the store’s core server are identified by that unique terminal ID” (col 10, lines 30-33), thus maintaining

Art Unit: 3622

anonymity of the customer. The Examiner notes that Ogasawara also discloses an embodiment in which “each customer is issued a unique customer ID which may be used by the mobile terminal ... such that transmissions between a mobile terminal and the store’s core server can be allocated to a particular customer” (col 10, lines 33-37). However, as Ogasawara points out, this is an alternative embodiment to the first disclosed embodiments which only uses the terminal ID. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made for Stewart to use the remote device ID by itself to only identify the remote device and its location without being able to further identify the specific user of the remote device; in other words, to eliminate the need for pre-registering the user. One would have been motivated to eliminate the system’s ability to identify the specific user in view of Stewart’s embodiment for presenting the promotions about the hotel in which the remote device was located; thus, eliminating the requirement to pre-register the user. One would find utility of such a system in large gatherings such as conventions in which a large number of users would be unfamiliar with the area but who would desire information about the surrounding facilities only for the few days that the convention was running.

Claims 36 and 37: Stewart and Ogasawara disclose a method for secure coupon distribution as in Claim 26 above, but do not explicitly disclose that the coupon data is encrypted before it is sent to the client system nor that the client system will also encrypt the coupon data upon receiving the data from the remote server. Official Notice

Art Unit: 3622

is taken that it is old and well known within the computer and data encryption arts to encrypt data being sent over unsecured networks using a plurality of encryption methods in order to provide a higher level of security to the data. In support of this Official Notice the Examiner previously provided Chapter 15 from a cryptography textbook from 1996 to show that not only was double encryption a well known method to further protect data, but triple encryption and other multiple encryption schemes were also well known and used in the art (Schneier, "Applied Cryptography, Second Edition", 1996, pp 357-368). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the coupon data in Stewart prior to transmitting the data over an unsecured network, such as the Internet as disclosed by Stewart, in order to prevent unauthorized interception of the data. It also would have been obvious to one having ordinary skill in the art at the time the invention was made to use a local encryption method to further encrypt and protect the encrypted data received from the remote server. One would have been motivated to further encrypt the coupon data in Stewart locally in this manner in order to prevent unauthorized disclosure of the selected coupons to other persons who may use the client device (e.g. other family members, co-workers, etc.).

Claim 38: Stewart and Ogasawara disclose a method for secure coupon distribution as in Claim 37 above, and Stewart further discloses generating a printed version of the transmitted coupon (print documents)(col 2, lines 36-47). It is inherent



Art Unit: 3622

that the client device must decrypt the encrypted coupon data before printing the coupon.

9. Claims 27-35, 39-43, 45, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart (5,835,601) in view of Ogasawara (6,123,259) and in further view of Barnett et al(6,321,208).

Claims 27 and 45: Stewart and Ogasawara disclose a system and method for secure coupon distribution as in Claim 26 above, but do not explicitly disclose that the device information includes at least one of a postal zip code associated with the user and a state in which the user reside. However, Barnett discloses a similar method for distributing coupons and further discloses the device information including at least one of a postal zip code and a state in which the user resides (col 4, lines 8-16 and 34-37). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include Stewart's user's zip code or state as information associated with the device. One would have been motivated to include such information in order to better target the selected coupon and in view of Stewart's disclosure of identifying the location of the remote device.

Claims 28 and 46: Stewart, Ogasawara, and Barnett disclose a system and method for secure coupon distribution as in Claims 27 and 45 above, and Stewart further discloses associating the device ID with a remote client system (col 4, lines 1-3).

Claim 29: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 28 above, and Stewart further discloses generating a printed version of the transmitted coupon (print documents)(col 2, lines 36-47).

Claim 30: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 28 above and Stewart further discloses the client device submitting a request including the device ID to the server (col 4, line 66 – col 5, line 6).

Claim 31: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 30 above, and Stewart further discloses automatically including the device ID without intervention by the user (col 5, lines 34-39 and col 9, lines 29-33).

Claim 32: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 30 above, and Stewart further discloses the request is automatically transmitted without intervention by the user (col 5, lines 34-39 and col 9, lines 29-33).

Claim 33: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 32 above, and Stewart further discloses the transmitting step occurs at predetermined intervals (beacon signals)(col 4, lines 10-19).

Art Unit: 3622

Claims 34 and 35: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 28 above, but do not explicitly disclose that the graphical user interface on the client device uses icons which may also flash to indicate the availability of new coupons. However, Official Notice is again taken that the use of icons, graphics, colors, animation, etc. to attract the viewer's attention on graphical user interfaces is well known in the computer arts, and their use would have been obvious to one having ordinary skill in the art at the time the invention was made. In support of this Official Notice, the Examiner previously provided excerpts from two HTML textbooks from 1996 to show that, not only was it well known to "flash" parts of a web page to attract the user's attention, but that the "Blink" command was also one of the standard commands in the programming language (Graham, "The HTML Sourcebook, Second Edition, A Complete Guide of HTML 3.0", 1996, pp 233-234)(Lemay, "Teach Yourself Web Publishing with HTML 3.0 in a Week", 1996, pp 183). Therefore, one would have been motivated to use icons, flashing or otherwise, to notify the user of the Stewart system in order to attract their attention more easily.

Claim 39: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 28 above, and Stewart further discloses displaying at least a portion of the advertisement (coupon) to the user of the client device (col 4, lines 5-7 and col 7, lines 12-20).

Claim 40: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 39 above, and Barnett further discloses selecting one of the plurality of coupons as a function of a selected subcategory of coupons available on the client system (col 10, lines 1-16). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to select the coupons in Stewart using categories and subcategories of coupons. One would have been motivated to sort the available coupons in this manner in order to preclude the user from having to look through hundreds or even thousands of coupons when attempting to locate one for a specific product.

Claim 41: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 28 above, and Barnett further discloses tracking the user's actions on the client device and maintaining a database at the main server of coupons selected and redeemed by the user (col 10, lines 51-57). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to track user's actions in Stewart and to record the coupons selected and redeemed by Stewart's user. One would have been motivated to store this tracking information in order to provide feedback to the advertisers, merchants, manufacturers, and other coupon issuers on the effectiveness and popularity of their product.

Claim 42: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 28 above, and Barnett further discloses determining a sponsor identification of a displayed coupon (col 11, lines 25-29). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine the sponsorship of the coupons being displayed to the user in Stewart. One would have been motivated to determine the sponsorship of the coupon in order to facilitate the billing of the sponsor, such as is common in the advertising arts.

Claim 43: Stewart, Ogasawara, and Barnett disclose a method for secure coupon distribution as in Claim 41 above. While it is not explicitly disclosed that the data being sent to the main server about the tracked user's actions is encrypted, it would have been obvious to do so for the same reasons discussed in reference to Claims 36 and 37 above.

### ***Response to Arguments***

10. Applicant's arguments with respect to claims 1-18 and 22-46 have been considered but are moot in view of the new ground(s) of rejection.

Applicant requested clarification of the status of the Schreiber and Mankoff references cited in a previous Office Action. As the Applicant has indicated, the Walsh memorandum, previously provided, established that the Applicant antedates both of these references. As such, these references were been removed from the rejections in both the previous and the above rejections.

***Conclusion***

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Sada (JP 2002/298052)(with English Abstract) discloses a system and method for distributing coupons to a user terminal which is identified by a user terminal identification (UID).

b. Gupta et al (5,361,871) discloses a system and method for coupon distribution to remote units identified by device IDs and further discloses that the remote devices can be issued to shoppers who do not have enough credit history, i.e. do not have a credit card to use as identification of the shopper.

c. Begum et al (5,420,606) discloses a system and method for distributing coupons to a remote device without being able to identify the user of the remote device.

d. Larson et al (5,708,782) discloses a system and method for distributing coupons to remote devices in conjunction with shopping carts.

e. O'Hagan et al (5,821,512) discloses a system and method for distributing promotions to a remote device mounted on a shopping cart which is able to print a selected coupon.

f. Duvall et al (5,884,033) discloses a system and method for filtering access to specific URLs (webpages).

g. Sloane (5,918,211) discloses a system and method for a handheld device which identifies promotions pertaining to scanned items without being able to identify the user of the handheld device.

h. Jelen et al (6,129,276) discloses a system and method for distributing to and printing promotions on remote devices mounted on shopping carts.

i. Sloane et al (6,434,530) discloses a system and method for a handheld device which identifies promotions pertaining to scanned items without being able to identify the user of the handheld device.

j. Blaeuer (6,484,939) discloses a system and method for distributing and printing coupons for a user of a shopping cart mounted device.

k. McNicol et al (6,615,179) discloses a system and method for distributing promotional material to users of handheld computers based on their location.

l. Tyler et al (6,638,316) discloses a system and method which identifies the source URL associated with requested information and allows or disallows (blocks) connection thereto by the user.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Exr. James W. Myhre whose telephone number is (703) 308-7843. The examiner can normally be reached Monday through Thursday from 6:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eric Stamber, can be reached on (703) 305-8469. The fax phone number for Formal or Official faxes to Technology Center 3600 is (703) 872-9306. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (703) 746-5544.

Note: Effective April 2005, the examiner's telephone numbers will be changed to (571) 272-6722 (phone) and (571) 273-6772 (Informal faxes); and the examiner's supervisor's telephone number will be changed to (571) 272-6724.



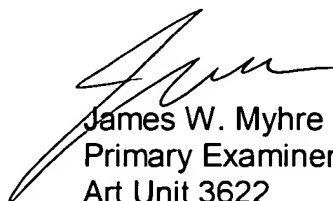
Art Unit: 3622

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (703) 308-1113.



JWM

February 10, 2005



James W. Myhre

Primary Examiner

Art Unit 3622